II LICEUM OGÓLNOKSZTAŁCĄCE
IM. KRÓLA JANA III SOBIESKIEGO
W KRAKOWIE

Piotr Bury

Elementy algebry z teorią liczb

Skrypt do zajęć
w roku szkolnym 2023/24

(Ostania aktualizacja: 12.06.2023)

KRAKÓW 2023

Matematykiem jest ten, dla kogo wzór: $\int\limits_{-\infty}^{+\infty} e^{-x^2}\,dx = \sqrt{\pi}$ *jest tak oczywisty,*
jak dla innych dwa razy dwa równa się cztery.

William Thomson

Spis treści

Wstęp

W drugim semestrze roku szkolnego 2019/20 miałem okazję prowadzić po raz pierwszy uzupełnienie *Elementy algebry z teorią liczb*. Przedmiot ten miał dość nietypowy syllabus – liczby zespolone, teorię grup, teorię relacji oraz nierówności między średnimi. Tematy te nie dotyczą w ogóle teorii liczb, a są związane zarówno z algebrą liniową, jak i abstrakcyjną. Znajdziemy tam również elementy teorii mnogości i analizy. W następnym roku szkolnym również powierzono mi prowadzenie tego przedmiotu, lecz nie tylko dla zwykłych klas z rozszerzoną matematyką, ale także dla klasy $M+$. Wymagania przedmiotowe w większości pokrywają się – różnicą jest ostatni dział. Zamiast nierówności omawiana jest relacja przystawania modulo, która jest częścią teorii liczb. Taka różnorodność zagadnień sprawia, że nie ma niestety żadnego podręcznika, czy zbioru zadań, który obejmowałby wszystkie wspomniane wyżej zagadnienia. Zarówno dla osób prowadzących zajęcia, jak i uczniów jest to spore utrudnienie – odpowiednich zadań trzeba szukać po wielu książkach lub wymyślać samemu. Opisana sytuacja była dla mnie głównym motywem, by taki skrypt powstał. Po zakończeniu roku szkolnego 2019/20 postanowiłem zebrać i przejrzeć swoje notatki, które wykorzystywałem podczas prowadzenia zajęć. Odpowiednio je posegregowałem, zredagowałem i w taki właśnie sposób powstał tenże skrypt, który zawiera zarówno pełną teorię z wprowadzanych przeze mnie zagadnień, jak i dość dokładnie wybrany zestaw zadań. Drugi rok prowadzenia tego przedmiotu pozwolił wyłapać drobne literówki, ujednolicić oznaczenia i wprowadzić zmiany, których konieczność dostrzegło się dopiero przy ponownym omawianiu tych samych zagadnień. Po wielu przemyśleniach postanowiłem też usunąć tematy związane z nierównościami między średnimi i tożsamościami[1], a w zamian umieściłem typowy dział algebry liniowej – macierze. Jest to zagadnienie, z którym praktycznie każdy spotka się już na pierwszym roku studiów, a więc poznanie tychże pojęć wcześniej na pewno będzie przydatne.

Skrypt jest napisany w taki sposób, by widoczna była przejrzysta struktura: najpierw przedstawiona jest teoria z wszystkich działów wraz z przykładami (podręcznik), a następnie znajdują się zadania, również podzielone na odpowiednie działy (zbiór zadań). Całość dopełniają odpowiedzi do wszystkich zadań, dzięki czemu zarówno nauczyciel prowadzący lekcję, jak i uczeń może sprawdzić, czy otrzymał poprawny wynik. Na samym końcu umieściłem *Dodatek*, w którym znajdują się zagadnienia uzupełniające. Są to takie zagadnienia, które uważam za wyjątkowo ciekawe, a które nie są objęte programem tego przedmiotu. Do zrozumienia większości z nich wystarczy dobra znajomość liczb zespolonych. Można je wykorzystać do pracy z uczniem zdolnym, wyróżniającym się na tle klasy, chcącym poznać coś więcej niż wiedza przekazywana na lekcji.

Dość długo zastanawiałem się, czy jest jakiś wspólny czynnik łączący tak różnorodne tematy. Ku mojej radości, taki element udało się znaleźć. Omawiane tutaj teorie (liczby zespolone, grupy, relacje, kongruencja, macierze) są pewnym uogólnieniem tego, co uczniowie poznają w na lekcjach matematyki. I tak po kolei:

[1] Tematy te są omawiane na lekcjach matematyki.

- Liczby zespolone są rozszerzeniem maksymalnego zbioru liczbowego jaki do tej pory poznaliśmy tzn. zbioru liczb rzeczywistych $\mathbb{R}$. Na początku naszej edukacji poznajemy zbiór liczb naturalnych, następnie „większy" zbiór liczb całkowitych, potem zbiór liczb wymiernych i na końcu rzeczywistych. Wydaje się, że to już koniec, bo każdy punkt na prostej możemy utożsamiać z liczbą rzeczywistą i na odwrót. Okazuje się jednak, że jest zbiór jeszcze „szerszy" i co więcej jest on w pewnym sensie idealny – każdy wielomian stopnia niezerowego ma pierwiastek[2] (!), co w oczywisty sposób nie zachodzi w $\mathbb{R}$.

- Grupy i działania w nich są uogólnieniem naturalnego działania dodawania i mnożenia w zbiorach takich jak np. $\mathbb{Z}$, czy $\mathbb{R}$ i zachodzących tam własności. Rozważając własności tych działań takie jak chociażby łączność, przemienność zastanawiamy się, jakie inne działania mają podobne własności. Okazuje się więc, że poznane już w szkole podstawowej mnożenie i dodawanie to nie jedyne naturalne działania. Są one jedynie przykładami znacznie szerszej, abstrakcyjnej teorii.

- Teoria relacji jest zaś na pewien sposób uogólnieniem pojęć związanych z funkcjami. Definicja funkcji, jaką poznajemy na lekcjach matematyki, jest co prawda intuicyjna i łatwa, ale nie jest niestety ścisła i formalna, więc w matematyce wyższej potrzebna jest inna. Tam właśnie wykorzystuje się teorię relacji. Funkcja znana z lekcji matematyki to przyporządkowanie mające specjalne własności. W szczególności możemy różnym argumentom przypisywać te same wartości[3], ale nie możemy jednemu elementowi przypisać dwóch różnych wartości. W przypadku relacji odrzucamy to ograniczenie, a więc intuicyjnie relacja to po prostu dowolne przyporządkowanie pomiędzy elementami pewnych zbiorów.

- Macierze to naturalne uogólnienie wektorów. Wiele intuicji się przenosi, tzn. będziemy takie macierze dodawać, mnożyć przez liczbę, czy też mnożyć przez siebie. Jak pamiętamy z lekcji matematyki, wektor w układzie współrzędnych był reprezentowany przez parę liczb np. $[2, 1]$. Macierz to taki „wielowskaźnikowy" wektor – składa się nie tylko z jedno wiersza, ale z kilku. Sam wektor $[2, 1]$ jest również macierzą – ma jeden wiersz i dwie kolumny.

- Relacja przystawania modulo (inaczej kongruencja) to narzędzie, które znacząco ułatwia pewne rzeczy związane z podzielnością liczb całkowitych. Dzięki niej badanie ogromnych liczb staje się prostsze, bo pozwala zajmować się jedynie ich resztami z dzielenia przez daną liczbę. Odpowiednie działania (jak np. mnożenie, dodawanie) wykonuje się na stosunkowo małym zbiorze reszt, a wnioski z nich wyciągane dotyczą liczb tak ogromnych, że niemożliwym byłoby nawet ich zapisanie.

Tekst został złożony w całości przy użyciu środowiska LaTeXw edytorze Texmaker. Wszystkie obrazki zawarte w skrypcie zostały wykonane przeze mnie osobiście w programie GeoGebra.

Jak w każdej publikacji, również i w tej, na pewno nie udało się uniknąć błędów: literówek, błędów redakcyjnych, czy też typograficznych. Dołożyłem wszelkich starań, by takie błędy się nie pojawiały, wielokrotnie sprawdzając napisany tekst. W przypadku zauważenia jakiegoś błędu proszę o bezpośredni kontakt. Skrypt będzie na bieżąco poprawiany i aktualizowany.

[2]Mówimy wtedy o **algebraicznej domkniętości** takiego zbioru.
[3]Wtedy po prostu funkcja nie jest różnowartościowa.

Rozdział 1

Teoria

1.1 Liczby zespolone

Definicja 1.1.1.
Niech A, B będą zbiorami. Definiujemy ***iloczyn kartezjański***[4] *zbiorów A i B jako:*

$$A \times B := \{(a,b) : \ a \in A \wedge b \in B\}.$$

Definicja 1.1.2.
Zbiorem liczb zespolonych[5] *nazywamy zbiór $\mathbb{C} := \mathbb{R} \times \mathbb{R}$.*

Uwaga 1.1.3.
Każdą liczbę zespoloną z możemy więc zapisać w postaci $z = (a,b)$, gdzie $a, b \in \mathbb{R}$.

Definicja 1.1.4 (Działania w $\mathbb{C}$)**.**

- $(a,b) + (c,d) := (a+c, b+d)$
- $(a,b) - (c,d) := (a-c, b-d)$
- $(a,b) \cdot (c,d) := (ac - bd, ad + bc)$

Definicja 1.1.5.
Liczbę $(0,1)$ nazywamy ***jednostką urojoną*** *i oznaczamy symbolem i.*[6]

[4] Pojęciem tym zajmiemy się dokładniej w rozdziale poświęconym teorii relacji. W tej chwili definicja ta jest nam potrzebna tylko po to, by zdefiniować zbiór liczb zespolonych.

[5] Szczególną uwagę należy zwrócić na oznaczenie tego zbioru. Używamy w tym celu litery C od słowa ***complex*** – w języku angielskim zbiór ten nazywa się *complex numbers*. Nie należy mylić oznaczenia z niepoprawnym oznaczeniem $\mathbb{C}$ na zbiór liczb całkowitych. Problem oznaczania zbioru liczb całkowitych przez $\mathbb{C}$ zamiast $\mathbb{Z}$ występował w polskich szkołach przez ostatnich kilkadziesiąt lat. Niejasność ta powinna zniknąć wraz z początkiem roku 2018, uwagi na fakt, że w *Rozporządzeniu Ministra Edukacji Narodowej z dnia 30 stycznia 2018 roku w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia* na stronie 293 czytamy, że uczeń powinien stosować prawidłowe i powszechnie przyjęte oznaczenia tzn. $\mathbb{Z}$ dla zbioru liczb całkowitych oraz $\mathbb{Q}$ dla zbioru liczb wymiernych. Niestety problem obecnie nadal występuje i niepoprawne oznaczenia możemy spotkać w wielu podręcznikach.

[6] Fizycy, elektrycy i osoby zajmujące się dziedzinami pokrewnymi często stosują oznaczenie j na jednostkę urojoną, ze względu, że literę i wykorzystują do innych celów np. do oznaczenia chwilowego natężenia prądu elektrycznego.

Zastanówmy się teraz, ile wynosi i^2.
$i^2 = (0,1)^2 = (0,1) \cdot (0,1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0)$.

Uwaga 1.1.6.
Każdą liczbę rzeczywistą a będziemy traktować jako liczbę zespoloną $(a, 0)$, tzn. $a = (a, 0)$.

Przy powyższym utożsamieniu otrzymujemy, że:

$$\boxed{\boldsymbol{i^2 = -1}}\,^{7}.$$

Zauważmy teraz, że dla każdego $a, b \in \mathbb{R}$ zachodzi:
$(a,b) = (a,0) + (0,b) \overset{\text{Ćw.}}{=} (a,0) + (b,0) \cdot (0,1) = a + bi$.
Powyższą postać tzn. $a + bi$ nazywamy **postacią algebraiczną (kanoniczną[8])** liczby zespolonej. Postać ta znacząco ułatwia rachunki, ponieważ pozwala traktować liczby zespolone jako wyrażenia algebraiczne – pamiętać należy jedynie, że $i^2 = -1$. Istotnie:
$(a + bi) + (c + di) = a + c + (b + d)i = (a + c, b + d)$,
$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = ac + (ad + bc)i - bd = ac - bd + (ad + bc)i = (ac - bd, ad + bc)$.

Definicja 1.1.7.
*Liczby postaci $0 + bi$ $(b \in \mathbb{R})$ nazywamy liczbami **urojonymi**.*

Definicja 1.1.8.
Niech $z = a + bi$, $a, b \in \mathbb{R}$. Definiujemy:

- $\operatorname{Re} z := a$ – ***część rzeczywista*** *liczby z,*
- $\operatorname{Im} z := b$ – ***część urojona*** *liczby z,*
- $\overline{z} := a - bi$ – ***liczba sprzężona*** *do z,*
- $|z| := \sqrt{a^2 + b^2}$ – ***moduł***[9] *liczby z.*

Twierdzenie 1.1.9.
$\forall z \in \mathbb{C}: \; z \cdot \overline{z} = |z|^2$.

Dowód. Ćwiczenie □

Definicja 1.1.10 (Dzielenie liczb zespolonych)**.**
Dla $z_1, z_2 \in \mathbb{C}, z_2 \neq 0$ definiujemy:
$$\frac{z_1}{z_2} := \frac{z_1}{z_2} \cdot \frac{\overline{z_2}}{\overline{z_2}} = \frac{z_1 \cdot \overline{z_2}}{|z_2|^2}.$$

[7] Mimo prawdziwej równości $i^2 = -1$ należy wystrzegać się dość popularnego zapisu, że $i = \sqrt{-1}$. Powody unikania tego zapisu są dwa: po pierwsze pierwiastek zespolony to zbiór, a nie liczba (o czym przekonamy się za chwilę), a po drugie taki pierwiastek nie ma typowych własności znanych ze zbioru liczb rzeczywistych. Stosowanie tego zapisu dość szybko prowadzi do błędów, jak chociażby udowodnienia, że $1 = -1$. Więcej na ten temat w Dodatku.
[8] Czasem nazywaną też postacią kanoniczną Gaussa.
[9] Jest to uogólnienie dobrze znanej wartości bezwzględnej ze zbioru liczb rzeczywistych.